VENABLE LLP
Jean-Paul P. Cart (SBN 267516)
jpcart@venable.com
Jonathan A. Mireles (SBN 339295)
jamireles@venable.com
Harry Libarle (SBN 346020)
hlibarle@venable.com
101 California Street, Suite 3800
San Francisco, CA 94111
Telephone: 415.653.3750
Facsimile: 415.653.3755

Attorneys for Defendant,
InMarket Media, LLC

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

IN RE INMARKET MEDIA LOCATION DATA TRACKING LITIGATION

Case No. 3:24-cv-00511-JSC

Hon. Jacqueline Scott Corley

DEFENDANT INMARKET MEDIA, LLC'S REPLY IN SUPPORT OF MOTION TO DISMISS CONSOLIDATED AMENDED CLASS ACTION COMPLAINT

Date: November 7, 2024
Time: 10:00 a.m.
Dept: 8, 19th Floor
Judge: Hon. Jacqueline Scott Corley

Action Filed: January 26, 2024
Trial Date: None

VENABLE LLP
101 CALIFORNIA STREET, SUITE 3800
SAN FRANCISCO, CA 94111
415.653.3750

TABILE OF CONTENTS

TABLE OF AUTHORITIES

Page(s)

Cases

Statutes

VENABLE LLP
101 CALIFORNIA STREET, SUITE 3800
SAN FRANCISCO, CA 94111
415.653.3750

I. INTRODUCTION.

Plaintiffs Autry Willis and Kenneth Kruger's ("Plaintiffs") Opposition concedes all the relevant facts that warrant dismissal of their Consolidated Amended Class Action Complaint (the "Amended Complaint") against Defendant InMarket Media, LLC ("InMarket") in its entirety.

First, Plaintiffs' invasion of privacy claim fails because they concede that they downloaded unnamed third-party mobile phone applications that "request[ed] access to the location data generated by [their] device's operating system," and thus they knew these unnamed third-party applications collected geolocation information. (Am. Compl. ¶¶ 7, 10, 24). Plaintiffs further concede that these unnamed third-party mobile phone applications only sent their geolocation data to InMarket while they were using such applications (*id.* ¶¶ 7, 10), and not "almost incessantly" or when they were not interacting with the applications, as the authorities Plaintiffs rely on in their Opposition suggest. Plaintiffs also concede that InMarket received a "unique mobile device identifier" (*id.* ¶¶ 25, 28), and not that InMarket knew (or that it could have known) who they were or that InMarket could link any geolocation information it allegedly obtained to their names.

In other words, Plaintiffs cannot plausibly allege an invasion of privacy claim, nor have they plausibly alleged that InMarket's alleged "surreptitious" collection of their location data is "highly offensive" or "egregious" when they never claim they ever visited any purported "sensitive" locations or that the unnamed third-party mobile phone applications they allegedly downloaded or used were even of capable tracking, collecting, or storing such information. As such, Plaintiffs' invasion of privacy claim fails as a matter of law.

Second, Plaintiffs do not (and cannot) allege the InMarket SDK could somehow identify them via the unnamed third-party applications they allegedly downloaded and used or that there is a market for Plaintiffs' real-time location data, much less that any such market is one Plaintiffs could access to plausibly allege a claim under the California Computer Data Access and Fraud Act (the "CDAFA"). At most, Plaintiffs allege that InMarket received a "unique mobile device identifier," (Am. Compl. at ¶¶ 25, 28), but never do they allege that InMarket knew who they were or that it could link any geolocation information to their names. Accordingly, Plaintiffs' CDAFA claim fails as a matter of law.

Third, Plaintiffs' reliance on *Greenley v. Kochava, Inc.*, 684 F. Supp. 3d 1024 (S.D. Cal. 2023) and *Moody v. C2 Educ. Sys. Inc. et al.*, 2:24-cv-04249-RGK-SK, 2024 WL 3561367 (C.D. Cal. July 25, 2024) to support their argument that an embedded SDK software that allegedly collects geolocation data can constitute a pen register under California law is misplaced. As InMarket explains in greater detail below, not only are *Greenley* and *Moody* not binding on this Court, but unlike the plaintiffs in *Greenley* and *Moody* who alleged that the defendant received far more than location data, Plaintiffs here have not alleged (nor could they) that InMarket's SDK is capable of collecting data reflecting Plaintiffs' "spending habits" and purchasing decisions, "usernames," "emails and customer IDs," "search terms," "activities within an app," and other "specific communications" made by the Plaintiffs like the defendant in *Greenley* allegedly collected or that the location data allegedly collected by InMarket's SDK can somehow be matched to some database to uncover Plaintiffs' identities like the software the defendants in *Moody* purportedly used. Because no such allegations exist in the Amended Complaint, Plaintiffs' cited authority does nothing to change the analysis outlined in InMarket's Motion (*see* Mot. at 17-18), and thus Plaintiffs fail to plausibly allege a claim under Cal. Penal Code § 638.51.

Fourth, Plaintiffs fail to plausibly allege any of the required elements necessary to establish a Section 631(a) claim brought under the "eavesdropping prong" of the California Invasion of Privacy Act ("CIPA"). Specifically, Plaintiffs' *single,* unsupported allegation that InMarket tracks activities such as "clicking a link, installing an app, selecting an option, or relaying a response," which appears to relate to Plaintiffs' allegations regarding InMarket's own (first party) application—that Plaintiffs do not allege they ever downloaded or interacted with—is insufficient to overcome well-settled authority from this District holding that automatically generated geolocation data does not constitute "content" susceptible to interception within the meaning of Section 631. Plaintiffs' allegation that InMarket collected geolocation information without their consent is also implausible because they fail to name which, if any, of the "over 300 third-party applications" (Opp. at 6) they purportedly downloaded and used, and thus InMarket (and this Court) is left to guess and speculate what disclosures, prompts, or information Plaintiffs were provided by the third-party mobile applications they purportedly downloaded. As to the third

requirement necessary to establish a Section 631(a) eavesdropping claim, courts in this District have repeatedly held that geolocation data is record information and not content within the meaning of Section 631, and thus no "messages" could have been intercepted while "'in transit,' or passing over a wire, or being sent or received from within California," as Section 631 requires. Finally, because geolocation data is not content under Section 631, Plaintiffs' argument that InMarket uses the "content" of the eavesdropped communications also fails.

Fifth, Plaintiffs' unjust enrichment claim fails as a matter of law because the majority of state and federal district courts in California do not recognize unjust enrichment as a freestanding claim. But, even if this Court finds that a standalone cause of action for unjust enrichment is available as a quasi-contract claim for restitution as Plaintiffs contemplate, there are no allegations in the Amended Complaint regarding any "benefit" that Plaintiffs *voluntarily* "conferred" on InMarket or that InMarket *induced* Plaintiffs to confer a benefit through mistake, fraud, or coercion as is required to establish a quasi-contract claim for restitution. Therefore, Plaintiffs' unjust enrichment claim also fails on this basis alone.

Finally, Plaintiffs fail to distinguish authority from this District holding that no federal court has wedged individual digital data into the California's Unfair Competition Law's (the "UCL") "money or property" box and contradictorily argue that they lost "money or property" within the meaning of the UCL because "the location data that Defendant surreptitiously took from them [] 'has monetary value for which they were not paid.'" (Opp. at 20.) More importantly, Plaintiffs' Opposition fails to address any of InMarket's other arguments for dismissal of Plaintiffs' UCL claims, and thus Plaintiffs concede these arguments by failing to oppose them. Instead, they simply request a second attempt at pleading their UCL claims without articulating any facts that they could plead to overcome the deficiencies outlined in InMarket's Motion. The Court should dismiss Plaintiffs' UCL claims and deny their request for leave to amend as futile.

II. ARGUMENT.

A. Plaintiffs' Invasion of Privacy Claim Fails as a Matter of Law.

Plaintiffs first argue they plausibly alleged a claim for invasion of privacy under the California Constitution and common law privacy rights because they have a reasonable and

protectable privacy interest in their geolocation data. (*See* Opp. 7-10.) Plaintiffs cite several Supreme Court and Ninth Circuit cases purportedly for the proposition that individuals have a reasonable expectation of privacy in the "the record of [their] physical movements," in the "contents of their cellphones," and against the collection of "broad swaths of person information absent consent." (*Id.* at 7 (citing *Carpenter v. United States*, 585 U.S. 296 (2018); *Riley v. California*, 573 U.S. 373 (2014); and *In re Facebook, Inc. Internet Tracking Litig.*, 956 F.3d 589, 601 (9th Cir. 2020).) But those are not the facts in the instant action. Specifically, Plaintiffs here do not allege that InMarket records users' phone calls or text messages or other sensitive information—and any communications at all—nor that InMarket collects an enormous amount of individualized data. Rather, Plaintiffs argue that InMarket "secretly gathers, aggregates, and sells vast amounts of **time-stamped, precise geolocation data from consumers' cell phones** without their consent," an allegation tied to InMarket's overall activities rather than the amount of data collected regarding any particular individual. (Opp. at 2.)

Plaintiffs rely heavily on *In re Google Location History Litig.* ("*Google*") in which the Court held that users of several of Google's applications (*e.g.*, Google Maps and Google Hangout) had a reasonable and protectable privacy interest in their location data when the plaintiffs alleged that Google tracked their location data "almost incessantly" even when a user was not interacting with any of Google's applications and even when the applications at issue in that action had nothing to do with a user's location such as music streaming, payment services, and social networking. 514 F. Supp. 3d 1147 (N.D. Cal. 2021). In other words, the *Google* Court found that the plaintiffs had a reasonable and protectable privacy interest in their location data when they plausibly alleged that the "proliferation of Google-hosted apps allows for a continuous flow of personal data to Google's servers, even when a user is not interacting with those apps" and even when user opted to turn "Location History off." *Id.* at 1155.

Critically, here, Plaintiffs concede that (1) they downloaded third-party applications that "request[ed] access to the location data generated by [their] device's operating system," and thus they knew these unnamed third-party applications collected geolocation information (Am. Compl. ¶¶ 7, 10, 24); (2) that these unnamed third-party applications only sent their geolocation data to

InMarket while they were using such applications (*id.* ¶¶ 7, 10), not "almost incessantly" and even when they were not interacting with the applications as the plaintiffs in *Google* alleged; and (3) that Plaintiffs contend that InMarket received a "unique mobile device identifier" (*id.* ¶¶ 25, 28), not that InMarket knew (or that it could have known) who they were or that InMarket could link any geolocation information it allegedly obtained to their names. Put differently, unlike in *Google*, Plaintiffs here do not similarly allege that InMarket's SDK or the third-party mobile applications they purportedly downloaded and used could collect and store such "comprehensive" and continuous information. As such, "Plaintiffs' allegations [here] are far too conclusory and speculative." *In re Google Location History Litig.*, 428 F. Supp 3d 185, 199 (N.D. Cal. 2019) ("Without more particular pleading, th[is] Court cannot determine if [defendant] extrapolated a 'mosaic' from the user data or if the data collected is 'sensitive and confidential' information.").

Plaintiffs further argue that InMarket's alleged surreptitious collection and dissemination of users' "personal and private whereabouts" is "highly offensive" or "egregious" because this data allows InMarket to track whether a user visited a doctor's office or attended a political rally, among other "sensitive" locations. (*See* Opp. at 10.) First, Plaintiffs never allege that they ever visited any such "sensitive" locations. But, more fundamentally, it is impossible to determine whether the undisclosed third-party mobile applications Plaintiffs allegedly downloaded and used can track, collect, or store such information as Plaintiffs fail—quite intentionally, mind you—to allege what applications they purportedly downloaded and used. Second, as InMarket explained in its Motion, Plaintiffs' overarching concern in the Amended Complaint is not that InMarket allegedly received geolocation information from their mobile devices, but rather that InMarket used that information to provide targeted advertisements to them—with such advertisements being displayed within the third-party application that provided the geolocation data. InMarket is still unaware of any legal authority—and Plaintiffs cite none—supporting the proposition that a desire to not be shown targeted advertisements constitutes a privacy interest, much less that a business's use of a narrow band of information to provide relevant advertising to a consumer within the confines of an advertising-supported mobile phone application is "highly offensive" conduct that reflects an "egregious" violation of societal norms.

Finally, Plaintiffs argue that they plausibly alleged that "InMarket intentionally and specifically designed its applications and its SDK to track Plaintiffs' location, affirmatively collected Plaintiffs' private data, took steps to aggregate that data, and then sold it for profit." (Opp. at 11 (citing Am. Compl. ¶¶ 4, 18-21, 27-30, 115, 136).) Not so. As InMarket explained in its Motion, Plaintiffs, at most, allege that InMarket "does little to verify" the disclosures made by third-party applications that provide geolocation data to InMarket. (Mot. at 15 (citing Am. Compl. ¶ 53).) The allegations in paragraphs 4, 18-21, 27-30, 115, 136 of the Amended Complaint do not establish otherwise.

B. Plaintiffs' CDAFA Claim Fails as a Matter of Law.

As Plaintiffs' own authority on this cause of action confirms, "[t]o bring a private civil cause of action under section 502, which is otherwise a criminal statute, a plaintiff must plead that he 'suffers damage or loss' due to the criminal violation." *Esparza v. Kohl's, Inc.*, No. 23-cv-01988-AJB-KSC, 2024 U.S. Dist. LEXIS 47564, at *18 (S.D. Cal. Mar. 18, 2024) (citing Cal. Penal Code § 502(e)). In *Esparza*, the Court found that plaintiff had "sufficiently allege[d] Defendant ha[d] a stake in the value of his misappropriated data" because plaintiff plausibly "allege[d] there is a market for his data that Defendant and ASI allegedly profit from" and defendant had "unfairly profited from secretly exploiting their ability to identify anonymous individuals who have visited Defendant's website." *Id.* (internal quotations omitted).

Plaintiffs here contend that "*Esparza* is instructive" because they similarly allege that InMarket was "unjustly enriched by intercepting, acquiring, taking, or using Plaintiffs' and Class Members' data, communications, and personal information without their permission, and using it for Defendant's own financial benefit." (Opp. at 12-13 (quoting Am. Compl. ¶ 96).) Plaintiffs further argue that they sufficiently alleged InMarket uses its "InMarket SDK spyware to access users' data and to monetize it by combining that data with data from other sources and selling it to advertisers." (*Id.* at 13 (citing Am. Compl. ¶¶ 31-52).) According to Plaintiffs, these allegations, collectively, are sufficient to state a claim under CDAFA. Not so.

Critically, unlike in *Esparza* where the defendant allegedly allowed a third party "to embed its chat technology code into the chat feature offered on Defendant's website" to enable

eavesdropping and that these "malware tools" allegedly "secretly install[] a 'persistent cookie' on every user's device" and "de-anonymizes website visitors," Plaintiffs here contend, at most, that the unnamed and unspecified third-party applications they allegedly downloaded and used containing InMarket's SDK tracked and collected their mobile device's geolocation data. In other words, Plaintiffs do not (and cannot) allege InMarket could somehow identify the anonymous individuals who download the unspecified third-party applications Plaintiffs allegedly downloaded or that there is a market for Plaintiffs' real-time location data, much less a market that they could conceivably access. In fact, Plaintiffs allege that InMarket received a "unique mobile device identifier," (*id.* at ¶¶ 25, 28), and never do they allege that InMarket knew who they were or that it could link any geolocation information to their names.[1]

Finally, Plaintiffs fail to distinguish InMarket's cited authority holding that when, as here, a plaintiff voluntarily gives permission to install some portion of a defendant's software, "any additional code installed at the same time was also installed with permission." *Flextronics Int'l, Ltd. v. Parametric Tech. Corp.*, No. 5:13-cv-00034-PSG, 2014 U.S. Dist. LEXIS 73354, at *15 & n.46 (N.D. Cal. May 28, 2014) ("[B]ecause [plaintiff] voluntarily gave permission to install some portion of [defendant's] software on its computers, any additional code installed at the same time was also installed with permission. This argument has been adopted in many other cases.") (collecting cases); *see also In re iPhone Application Litig.*, No. 11-MD-02250-LHK, 2011 WL 4403963, at *12 (N.D. Cal. Sep. 20, 2011) ("Plaintiffs have still failed to allege how Defendants can be liable for accessing Plaintiffs' computers 'without permission.' On Plaintiffs' own

[1] Plaintiffs' other cited authority on this issue is also distinguishable. *See Brown v. Google LLC*, 685 F. Supp. 3d 909, 940 (N.D. Cal. 2023) (holding that the Court could not "rule, as a matter of law, that plaintiffs suffered no damages under CDAFA" when "plaintiffs **proffer evidence that there is a market for their data**—one Google itself has created[.]") (emphasis added); *In re Facebook Inc. Internet Tracking Litig.*, 956 F.3d 589, 600 (9th Cir. 2020) (finding that plaintiffs had "adequately pleaded an entitlement to Facebook's profits from users' personal data sufficient to confer Article III standing" when plaintiffs alleged that "their browsing histories carry financial value" and by "**point[ing] to the existence of a study that values users' browsing histories at $52 per year, as well as research panels that pay participants for access to their browsing histories**.") (emphasis added); *Greenley v. Kochava, Inc.*, 684 F. Supp. 3d 1024 (S.D. Cal. 2023) (does not address what constitutes "damage or loss" under Cal. Penal Code § 502(e)(1)). Plaintiffs here make no such allegation that a market for their real-time location data exists.

allegations, the iOS and third-party apps— which contain the alleged 'surreptitious code'—were all installed or updated *voluntarily* by Plaintiffs.") (emphasis in original).

C. Plaintiffs' Cal. Penal Code § 638.51 Claim Fails as a Matter of Law.

Plaintiffs next argue that InMarket's SDK is a pen register because it "records addressing or signaling information—*i.e.*, Plaintiffs' and Class Members' location data and personal information—from the electronic communications transmitted over their smartphones" and because InMarket "did not obtain a court order permitting its use of the InMarket SDK spyware on Plaintiffs' and Class Members' devices." (Opp. at 14 (citing Am. Compl. ¶¶ 104-05).) In their Opposition, Plaintiffs rely almost exclusively on *Greenley v. Kochava, Inc.*, 684 F. Supp. 3d 1024 (S.D. Cal. 2023) and *Moody v. C2 Educ. Sys. Inc. et al.*, 2:24-cv-04249-RGK-SK, 2024 WL 3561367 (C.D. Cal. July 25, 2024) to support their argument that an embedded SDK software that allegedly collects geolocation data can constitute a pen register under California law. (*See* Opp. at 15.) However, as InMarket explained in its Motion (*see* Mot. at 17-18), *Greenley* is not binding on this Court, and contrary to Plaintiffs' assertion, *Greenley* is not "nearly identical to this [case]" (Opp. at 15) because unlike the plaintiffs in *Greenley* who alleged that the defendant received far more than location data through its SDK—that is, they alleged that the defendant received data reflecting their "spending habits" and purchasing decisions, "usernames," "emails and customer IDs," "search terms," "activities within an app," and other "specific communications" made by the plaintiffs, Plaintiffs here have not alleged that InMarket's SDK is capable of collecting such information. Thus, *Greenley* is not "nearly identical" and is, in fact, distinguishable because the data allegedly received in *Greenley* reflected communicative actions by the plaintiffs, such as what websites they visited and communicated with, and not merely where plaintiffs' phones were located at certain times as is the case here.

Similarly, in *Moody*, the "TikTok Software" at issue collected substantial amounts of data from anonymous visitors to the *Moody* defendant's website through a process called "fingerprinting," which included "device and browser information, geographic information, referral tracking, and URL tracking…[and a] user's name, date of birth, and address." *Moody v. C2 Educ. Sys.*, 2024 WL 3561367, at *1. But more important, and unlike the facts here, the data

collected by the defendant in *Moody* was then matched with TikTok's database to uncover the visitors' identities. *Id.* No such allegations exist in the Amended Complaint. Specifically, Plaintiffs allege only that InMarket received data from their mobile devices telling InMarket where the mobile device was located at a specific time, and thus *Moody* is distinguishable.

D. Plaintiffs' Cal. Penal Code § 631 Claim Fails as a Matter of Law.

Plaintiffs' Opposition confirms that their Section 631(a) claim is brought under the "eavesdropping prong" of the California Invasion of Privacy Act *only*. (*See* Opp. at 17-19.) Specifically, Plaintiffs contend that InMarket violated Section 631(a) of the California Penal Code by eavesdropping on Plaintiffs' communications and using those eavesdropped-upon communications.

As Plaintiffs' own authority explains, to plead a viable claim under the second clause of Section 631, Plaintiffs must allege that (1) InMarket "read, or attempt[ed] to read or to learn, the contents of a message or similar communication;" (2) without "the consent of 'all parties,' or in some other 'unauthorized manner;'" (3) that such conduct was "done while the message [wa]s 'in transit,' or passing over a wire, or being sent or received from within California;" and (4) such conduct was "willfully" done. *Valenzuela v. Nationwide Mut. Ins. Co.*, 686 F. Supp. 3d 969, 976-77 (C.D. Cal. 2023); Opp. at 17-18. Plaintiffs fail to establish any of these required elements.

First, under the federal Wiretap Act and CIPA,[2] "'content' is limited to information the user intended to communicate, such as the words spoken in a phone call." *In re iPhone Application Litig.*, 844 F. Supp. 2d 1040, 1061 (N.D. Cal. 2012). Courts in this District have repeatedly held that, like here, geolocation data that is "generated automatically, rather than through the intent of the user…does not constitute 'content' susceptible to interception." *Id.*; *Brodsky*, 445 F. Supp. 3d at 127 (holding that text messages are content, but "usernames, passwords, and geographic location information are not"); *Gonzales v. Uber Techs., Inc.*, 305 F. Supp. 3d 1078, 1085 (N.D. Cal. 2018) ("While a text message stating 'I am at 6th and Broadway' would constitute content, the automatic

[2] "The analysis for a violation of CIPA is the same as that under the federal Wiretap Act," and thus the definition of "contents" under the federal Wiretap Act applies to CIPA § 631(a) claims. *Brodsky v. Apple Inc.*, 445 F. Supp. 3d 110, 127 (N.D. Cal. 2020) (applying definition of "contents" under the federal Wiretap Act to CIPA § 631(a) claims).

generation of geolocation data is record information.") (internal citations omitted). "Cases holding that non-text information generated by CIPA plaintiffs constitutes intercepted 'contents' have chiefly focused on 'session replay' technologies, which capture video of the user's entire session," which simply is not the case here. *Jones v. Tonal Sys.*, No. 3:23-cv-1267-JES-BGS, 2024 U.S. Dist. LEXIS 178056, at *22-23 (S.D. Cal. Sept. 30, 2024) (dismissing "Second Prong — Eavesdropping" CIPA claim, in part, because plaintiff had "not met her burden to demonstrate that her 'engage[ment]' with the chat feature contained more than record information" when plaintiff alleged that defendant's software "can record…the full transcript of the conversation, the date and time the conversation began, the IP address of the visitor, the web browser they used to access the Website (Chrome, Firefox, etc.), [and] the device they used to have the chat conversation" and that defendant "can or may tag and organize users' conversations and route visitors to customer service agents or 'bot playbook[s],'" and defendant "uses cookies to track website visitor activity").

Here, Plaintiffs fail to acknowledge, much less distinguish, the above-cited authority. Instead, Plaintiffs simply argue in their Opposition that they plausibly alleged InMarket learned or attempted to learn of the contents of their communications because InMarket's "SDK communicates the user's affirmative actions, such as clicking a link, installing an app, selecting an option, or relaying a response, and constitute communications within the scope of the Wiretapping Act." (Am. Compl. ¶ 112.) However, besides this *single* and conclusory allegation, Plaintiffs provide no authority to support their argument that "clicking a link, installing an app, selecting an option, or relaying a response" constitute communications within the scope of CIPA. In short, Plaintiffs' unsupported allegation that InMarket tracks activities such as "clicking a link, installing an app, selecting an option, or relaying a response," which appears to relate to Plaintiffs' allegations regarding InMarket's own (first party) application—that Plaintiffs do not allege they ever downloaded or interacted with—is insufficient to overcome the express findings in *In re iPhone Application Litig.*, *Gonzales*, and *Brodsky* that automatically generated geolocation data does not constitute "content" susceptible to interception within the meaning of Section 631.

Second, Plaintiffs allege that InMarket violated Section 631 by "knowingly accessing and without permission accessing Plaintiffs and Class Members' devices in order to obtain their

personal information, including their device and location data and personal communications with others." (Opp. at 18 (citing Am. Compl. ¶¶ 128-29).) However, as InMarket explained in its Motion, "it is impossible to determine what disclosures, terms of use, or other relevant information Plaintiffs were potentially exposed to, read, and/or relied upon before downloading the applications and while allegedly using the relevant third-party application(s)" because Plaintiffs never disclose the specific applications they allegedly downloaded and used and on which their claims are based. (Mot. at 7 n.1.) Because Plaintiffs fail to name which, if any, of the "over 300 third-party applications" (Opp. at 6) they purportedly downloaded and used, InMarket (and this Court) is left to guess and speculate what disclosures, prompts, or information Plaintiffs were provided by the third-party mobile applications they purportedly downloaded, rendering implausible their allegation that InMarket collected geolocation information without their consent.

Third, because geolocation data is record information and not content within the meaning of Section 631, no "messages" could have been intercepted while "'in transit,' or passing over a wire, or being sent or received from within California," as Section 631 requires. *See Gonzales*, 305 F. Supp. 3d at 1085 ("Plaintiff's geolocation data is also record information rather than the content of a communication[.]"); *Brodsky*, 445 F. Supp. 3d at 127 (finding that text messages are content, but "geographic location information [is]not"); *In re iPhone Application Litig.*, 844 F. Supp. 2d at 1061 (holding that geolocation data that is "generated automatically, rather than through the intent of the user, does not constitute 'content' susceptible to interception").

Fourth, Plaintiffs argue that InMarket "acted willfully" in accessing their communications. (*See* Opp. at 19 (citing Am. Compl. ¶ 125).) However, again, geolocation data is record information, not content, messages, or communications within the meaning of Section 631. *See Gonzales*, 305 F. Supp. 3d at 1085; *Brodsky*, 445 F. Supp. 3d at 127; *In re iPhone Application Litig.*, 844 F. Supp. 2d at 1061. As such, InMarket could not have willfully (or otherwise) "read, or attempt[ed] to read or to learn" the "contents" of any "message" or "similar communication" because geolocation data is record information, not content, messages, or communications.

Finally, because geolocation data is not content under Section 631, Plaintiffs' further argument that InMarket uses the "content" of the eavesdropped communications also fails.

E. Plaintiffs' Unjust Enrichment Claim Fails as a Matter of Law.

As InMarket explained in its Motion, whether an independent cause of action based on unjust enrichment can be asserted is an unresolved question in the Ninth Circuit and among California courts, but "the more widely accepted principle [is] that there is no separate cause of action for unjust enrichment." *Blue Wing Airlines Fin. v. Unical Aviation, Inc.*, No. 8:22-cv-02052 JVS (ADSx), 2023 WL 3149276, at *2 n.2 (C.D. Cal. Mar. 8, 2023); *Baxter Bailey & Assocs. v. Ready Pac Foods, Inc.*, No. CV 18-08246-AB-GJSX, 2020 WL 1625257, at *6 (C.D. Cal. Feb. 26, 2020) (The "majority of state and federal district courts in California do not recognize unjust enrichment as a freestanding claim.") (quoting *Forcellati v. Hyland's, Inc.*, 876 F. Supp. 2d 1155, 1166-67 (C.D. Cal. 2012)). As such, Plaintiffs' claim should fail as a matter of law.

However, even if this Court finds that a standalone cause of action for unjust enrichment is available as a quasi-contract claim for restitution, restitution is not ordinarily available to a plaintiff unless "the benefits were conferred by mistake, fraud, coercion or request; otherwise, though there is enrichment, it is not unjust." *Nibbi Bros., Inc. v. Home Fed. Sav. & Loan Assn.*, 205 Cal. App. 3d 1415, 1422 (1988); *see also Bittel Technology, Inc. v. Bittel USA, Inc.*, No. 10-cv-00719, 2010 WL 3221864, at *5 (N.D. Cal. Aug. 13, 2010) ("[A] plaintiff must show that the benefit was conferred on the defendant through mistake, fraud, or coercion.") (citations omitted).

Here, Plaintiffs' allegation that InMarket "profited from their personal and private data" and that it "retains that benefit" is insufficient to state an unjust enrichment claim because Plaintiffs do not allege that any supposed benefit conferred on InMarket was "conferred by mistake, fraud, coercion or request." *Nibbi Bros., Inc.*, 205 Cal. App. 3d at 1422; *Bittel Technology, Inc.*, 2010 WL 3221864, at *5. Instead, Plaintiffs repeatedly argue that InMarket "surreptitiously" collected and profited from their location data. In other words, not only are there no allegations in the Amended Complaint regarding any "benefit" that Plaintiffs *voluntarily* "conferred" on InMarket, but an allegation that a defendant "surreptitiously" took something from a plaintiff with whom it had no contractual or quasi-contractual relationship is very different from an allegation that a defendant *induced* a plaintiff to confer a benefit through mistake, fraud, or coercion. Plaintiffs' conclusory and speculative allegation that InMarket "profited from their personal and private data"

and that it "retains that benefit" is insufficient to state a viable claim. *See Rosal v. First Fed. Bank of Cal.*, 671 F. Supp. 2d 1111, 1133 (N.D. Cal. 2009) ("conclusory allegation" that defendants "retain[ed] profits, income and ill-gotten gains at the expense of plaintiff" was "insufficient" to state a cause of action for "Restitution for Unjust Enrichment").

F. Plaintiffs' UCL Claims Fail, and Plaintiffs Provide No Supporting Facts, Arguments, or Authority for why Leave to Amend Should be Granted.

Plaintiffs argue that they lost "money or property" within the meaning of the UCL because "the location data that Defendant surreptitiously took from them [] 'has monetary value for which they were not paid.'" (Opp. at 20 (citing *Brown*, 685 F. Supp. 3d at 942).) However, Plaintiffs fail to distinguish this District's finding in *Rodriguez v. Google LLC*, No. 20-cv-04688-RS, 2021 WL 2026726, at *8 (N.D. Cal. May 21, 2021) that "no federal court has wedged individual digital data into the UCL's 'money or property' box," which explicitly contradicts their argument.

More important, however, Plaintiffs' Opposition fails to address any of InMarket's other arguments for dismissal of Plaintiffs' UCL claims, and thus Plaintiffs concede these arguments by failing to oppose them. *See Adam Askari D.D.S. Corp. v. U.S. Bancorp*, No. 5:21- CV-09750-EJD, 2022 WL 2161603, at *3 (N.D. Cal. June 15, 2022) (arguments are "conceded" if not opposed); *Tyler v. Travelers Com. Ins. Co.*, 499 F. Supp. 3d 693, 701 (N.D. Cal. 2020) ("As an initial matter, Plaintiff concedes these arguments by failing to address them in her opposition."); *Gordon v. Davenport*, No. 08-cv-3341, 2009 WL 322891, at *4 n.4 (N.D. Cal. Feb. 9, 2009) ("Indeed, plaintiff does not even address his third cause of action in his opposition brief, suggesting that he concedes defendants' assertion that he fails to state facts giving rise to a claim for relief.'), *aff'd sub nom. Gordon v. State Bar of Cal.*, 369 Fed. App'x. 833 (9th Cir. 2010); *Ramirez v. Ghilotti Bros. Inc.*, 941 F. Supp. 2d 1197, 1210 (N.D. Cal. 2013) (deeming argument conceded where plaintiff failed to address it in opposition); *Adams v. Starbucks Corp.*, No. SACV 20-00225 JVS (KESx), 2020 WL 4196248, at *6 (C.D. Cal. Jul. 9, 2020) (same).

Instead, Plaintiffs' Opposition simply requests a second bite at the apple and seeks leave for Plaintiffs to amend their UCL claims without explaining what, if any, proposed amendments or allegations Plaintiffs could provide or allege to cure the several defects InMarket identified in

its Motion. Because Plaintiffs fail to articulate any facts that they could plead to overcome the deficiencies outlined in InMarket's Motion, the Court should deny Plaintiffs' request for leave to amend because amendment would be futile. *See Kendall v. Visa U.S.A., Inc.*, 518 F.3d 1042, 1052 (9th Cir. 2008) (holding that "amendment would be futile" where the plaintiffs seeking leave to amend "fail to state what additional facts they would plead if given leave to amend"); *Chang v. Noh*, 787 F. App'x 466, 467 (9th Cir. 2019) (district court did "not abuse its discretion by denying request for leave to amend" when the plaintiff merely requested leave "in his opposition to the Rule 12(b)(6) motion" but "provided no supporting argument or authority for why leave to amend should be granted"); *Wysocki v. Zoom Techs. Inc.*, No. 3:22-cv-05453-DGE, 2024 WL 1139094, at *17 (W.D. Wash. Mar. 15, 2024) ("With no explanation as to how the complaint's deficiencies would be cured by amendment, the Court declines to grant leave to amend."); *see also Foskaris v. Experian Info. Sols., Inc.*, 808 F. App'x 436, 439–440 (9th Cir. 2020) ("It is not the court's duty, however, to peruse the record to formulate the parties' arguments.").

III. CONCLUSION.

For the foregoing reasons, InMarket respectfully requests that this Court grant its Motion in its entirely, without leave to amend.

Dated: October 7, 2024

VENABLE LLP

By: */s/ Jean-Paul P. Cart*
Jean-Paul P. Cart
Attorneys for Defendant,
InMarket Media, LLC